FortiAuthenticator™ VM Appliances

Install Guide

FortiAuthenticator™ VM Appliances Install Guide

October 19, 2014

Revision 2

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Change Log

Revision	Date	Change Description
1	2013-12-06	Initial Release
2	2014-10-16	Updated to include Microsoft Hyper-V

Introduction

The FortiAuthenticator device is an identity and access management solution. Identity and access management solutions are an important part of an enterprise network, providing access to protected network assets and tracking user activities to comply with security policies.

FortiAuthenticator provides user identity services to the Fortinet product range, as well as third party devices.

FortiAuthenticator delivers multiple features including:

- **Authentication:** FortiAuthenticator includes Remote Authentication Dial In User Service (RADIUS) and Lightweight Directory Access Protocol (LDAP) server authentication methods.
- **Two Factor Authentication:** FortiAuthenticator can act as a two-factor authentication server with support for one-time passwords using FortiToken 200, FortiToken Mobile, Short Message Service (SMS), or e-mail. FortiAuthenticator two-factor authentication is compatible with any system which supports RADIUS.
- **IEEE802.1X Support:** FortiAuthenticator supports 802.1X for use in FortiGate Wireless and Wired networks.
- **User Identification:** FortiAuthenticator can identify users through multiple data sources, including Active Directory, Desktop Client, Captive Portal Logon, RADIUS Accounting, Kerberos, and a Representational State Transfer (REST) API. It can then communicate this information to FortiGate, FortiCache, or FortiMail units for use in Identity Based Policies.
- **Certificate Management:** FortiAuthenticator can create and sign digital certificates for use, for example, in FortiAuthenticator VPNs and with the FortiToken 300 USB Certificate Store.
- **Integration:** FortiAuthenticator can integrate with third party RADIUS and LDAP authentication systems, allowing you to reuse existing information sources. The REST API can also be used to integrate with external provisioning systems.

Document scope

This document describes how to deploy a FortiAuthenticator virtual appliance in supported virtualization server environments. This includes how to configure the virtual hardware settings of the virtual appliance.

This document assumes:

- you have already successfully installed the virtualization server on the physical machine,
- you have installed appropriate VM management software on either the physical server or a computer to be used for VM management.

This document does not cover configuration and operation of the virtual appliance after it has been successfully installed and started. For these issues, see the *FortiAuthenticator Admin Guide*.

This document includes the following sections:

- FortiAuthenticator VM Overview
- Deployment example: VMware
- Deployment example: MS Hyper-V

FortiAuthenticator VM Overview

The following topics are included in this section:

FortiAuthenticator VM models and licensing

Fortinet offers the FortiAuthenticator VM in two virtual appliance models supporting VMWare and Microsoft Hyper-V hypervisors, which share a common stackable, perpetual license model. This model allows you to grow your VM solution as your environment expands. It is also possible to change between VM hypervisor using the same license key.

To license a FortiAuthenticator VM, purchase the correct multiple of licenses to meet your user requirements.

Table 1:- FortiAuthenticator VM license options

SKU	Description
FAC-VM-Base	Base FortiAuthenticator-VM with 100 user license. Unlimited vCPU
FAC-VM-100-UG	FortiAuthenticator-VM with 100 user license upgrade
FAC-VM-1000-UG	FortiAuthenticator-VM with 1000 user license upgrade
FAC-VM-10000-UG	FortiAuthenticator-VM with 10,000 user license upgrade
FAC-VM-100000-UG	FortiAuthenticator-VM with 100,000 user license upgrade

Note that the base license is ***always*** required e.g. for 43,000 users you would be required to purchase:

1 x FAC-VM-Base

3 x FAC-VM-1000-UG

4 x FAC-VM-10000-UG

Table 2:- FortiAuthenticator VM support options

SKU	Description
FC1-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–500 users)
FC2-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–1100 users)
FC3-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–5100 users)
FC4-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–10100 users)
FC5-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–50100 users)
FC6-10-0ACVM-248-02-12	1 Year 24x7 FortiCare Contract (1–100100 users)

Support is required for the total number of licensed users e.g. for 1 year support for 43,000 users, you would be required to purchase the 1 Year 24x7 FortiCare Contract (1–50100 users) contract.

When configuring your FortiAuthenticator VM, be sure to configure hardware settings within the ranges outlined in Table X and consider future expansion. Contact your Fortinet Authorized Reseller for more information,

Table 3:- FortiAuthenticator VM Specifications

Technical Specification	VM-BASE	VM-100-UG	VM-1000-UG	VM-10000-UG	VM-100000-UG
Virtual CPUs (Maximum)	Unlimited				
Virtual Network Interfaces (Min / Max)	1 / 4				
Virtual Memory (Min / Max)	512MB / 64GB				
Virtual Storage (Min / Max)	60 GB / 2 TB				
High Availability	Yes				
Local Users / Remote Users	100	+100	+1000	+10000	+1000000

FortiAuthenticator VM evaluation license

FortiAuthenticator VM includes a limited embedded 5 user license. This can be used for basic testing however no technical support is included. For formal product evaluations, please contact your Fortinet Authorized Reseller who can provide a fully supported 30 day trial license.

Registering FortiAuthenticator VM with Customer Service & Support

After placing an order for FortiAuthenticator VM, a license registration code is sent to the email address used in the purchase order form.

To obtain the FortiAuthenticator VM license file you must first register your FortiAuthenticator VM with Fortinet Customer Service & Support.

To register your FortiAuthenticator VM:

1. Log in to the Customer Service & Support portal using an existing support account or select *Sign Up* to create a new account.
2. In the main page, under Asset, select *Register/Renew*. The Registration page opens.
3. Enter the registration code that was emailed to you and select *Register*. A registration form will display.
4. Enter the IP address of the FortiAuthenticator VM. The license will be tied to this IP address.
5. After completing the form, a registration acknowledgement page will appear.
6. Select the *License File Download* link.
7. You will be prompted to save the license file (.lic) to your local computer. See “Upload the FortiAuthenticator VM license file” on page 45 for instructions on uploading the license file to your FortiAuthenticator VM via the Web-based Manager

You can configure basic network settings from the CLI to complete the deployment, ensuring the same IP address is configured as was used to register the VM. Once the license file is uploaded, the user count will be increased to the licensed number.

Downloading the FortiAuthenticator VM deployment package

FortiAuthenticator VM deployment packages are included with FortiAuthenticator firmware images on the Customer Service & Support site. First, see Table 2 to determine the appropriate VM deployment package for your VM platform. The firmware images FTP directory is organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention and each firmware image is specific to the device model.

Table 4:- Selecting the correct FortiAuthenticator VM deployment package for your VM platform

VM Platform	FortiAuthenticator VM Deployment File
VMware ESX 4.0, 4.1 VMware ESXi 4.0/4.1/5.0/5.1/5.5	FAC_VM-v300-buildxxxx-FORTINET.out.ovf.zip
Microsoft Hyper-V Server 2008R2 and 2012R2 Microsoft Server 2008R2 and 2012R2 Hyper-V	FAC_VM_HV-v300-buildxxxx-FORTINET.out.hyperv.zip

Note: Whilst provided in Open Virtualization Format (OVF), only VMWare ESXi is supported. Installation of this file on other hypervisor platforms is not supported.

Deployment package contents

VMware ESX/ESXi

The FAC_VM-v300-buildxxxx-FORTINET.out.ovf.zip file contains:

- fac.vmdk: the FortiAuthentication VM system hard disk in VMDK format
- datadrive.vmdk: the FortiAuthenticator VM log disk in VMDK format
- Open Virtualization Format (OVF) template files:
  - FortiAuthenticator-VM.ovf: OVF template file for VMware Hardware Type 10 (intel E1000 NIC Driver)
  - FortiAuthenticator-VM.hw07.ovf: OVF template file for VMware Hardware Type 7 (intel E1000 NIC Driver)
  - FortiAuthenticator-VM.hw04.ovf: OVF template file for VMware Hardware Type 7 (intel E1000 NIC Driver)

Microsoft Hyper-V

The FAC_VM_HV-v300-buildxxxx-FORTINET.out.hyperv.zipfile contains:

- In the Virtual Hard Disks folder:
  - fac.vhd: the FortiAuthenticator VM system hard disk in VHD format
  - DATADRIVE.vhd: the FortiAuthenticator VM log disk in VHD format
- In the Virtual Machines folder:
  - fortiauthentication.xml: XML file containing virtual hardware configuration settings for Hyper-V. This is compatible with Windows Server 2012R2.
- Snapshots folder: optionally, Hyper-V stores snapshots of the FortiAuthenticator VM state here

Deploying the FortiAuthenticator VM appliance

Prior to deploying the FortiAuthenticator VM appliance, the VM hypervisor platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiAuthenticator VM assume that this requirement has already been met and:

- you are familiar with the management software and terminology of your VM platform.
- an Internet connection is available for FortiAuthenticator VM to contact FortiGuard to validate its license

For assistance in deploying FortiAuthenticator VM, refer to the deployment chapter in this guide that corresponds to your VM hypervisor environment. You might also need to refer to the documentation provided with your VM server. The deployment chapters are presented as examples because for any particular VM server there are multiple ways to create a virtual machine. There are command line tools, APIs, and even alternative graphical user interface tools.

Before you start your FortiAuthenticator VM appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiAuthenticator VM, you will have access only through the console window of your VM server environment. After you configure one FortiAuthenticator network interface with an IP address and administrative access, you can access the FortiAuthenticator VM web-based manager.

After deployment and license validation, you can upgrade your FortiAuthenticator VM appliance firmware in a similar way to hardware by downloading the appropriate update file for your VM hypervisor:

VMWare ESXi	FAC_VM_HV-v300-buildxxxx-FORTINET.out
Microsoft Hyper-V	FAC_VM_HV-v300-buildxxxx-FORTINET.out

Deployment example: VMware

Once you have downloaded the FAC_VM-v300-buildxxxx-FORTINET.out.ovf.zip file and extracted the package contents to a folder on your local computer, you can use the vSphere client to create the virtual machine from the deployment package OVF template.

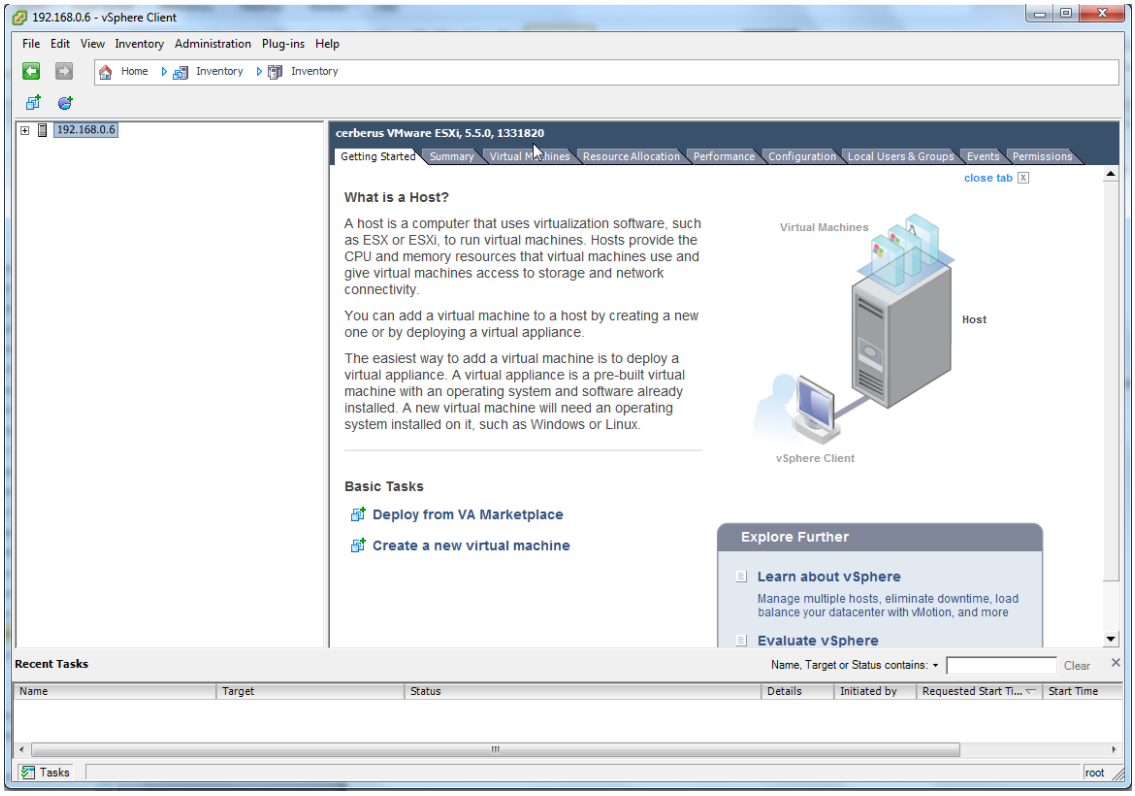
The following topics are included in this section:

- Open the FortiAuthenticator VM OVF file with the vSphere client
- Configure FortiAuthenticator VM hardware settings
- Power on your FortiAuthenticator VM

Open the FortiAuthenticator VM OVF file with the vSphere client

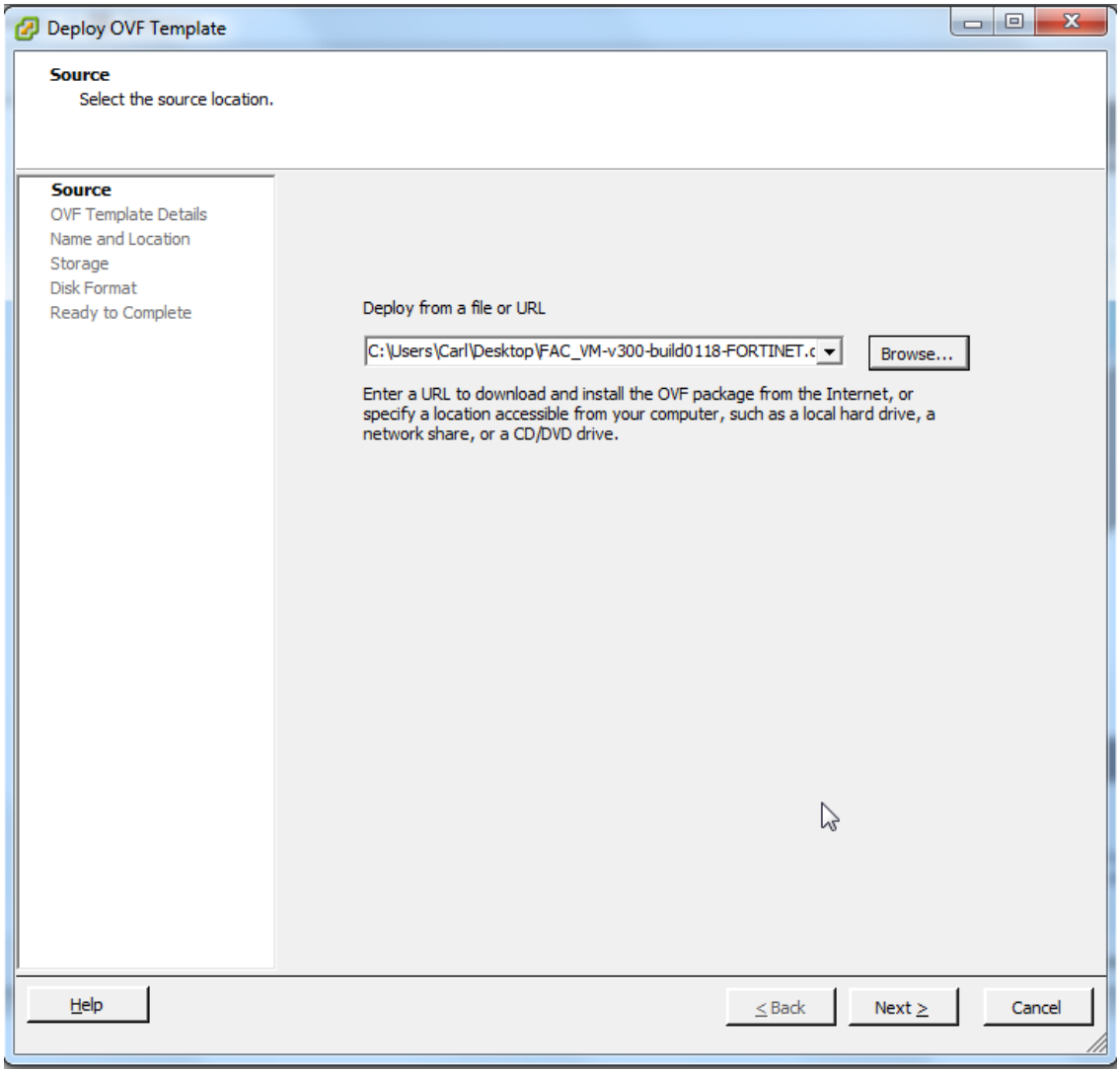
To deploy the FortiAuthenticator VM OVF template:

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password and select Login.

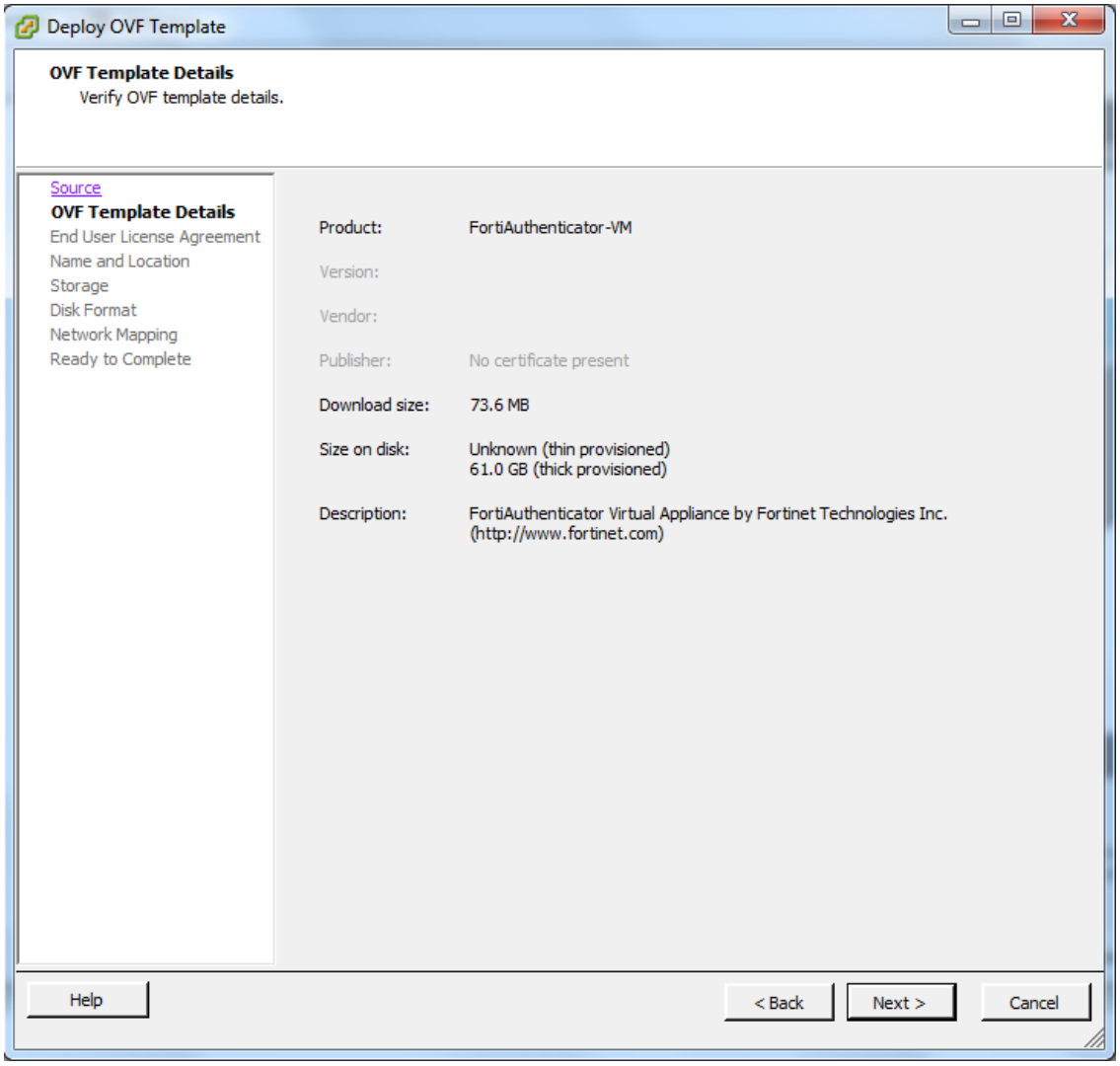


2. Select *File* > *Deploy OVF Template* to launch the OVF Template wizard.

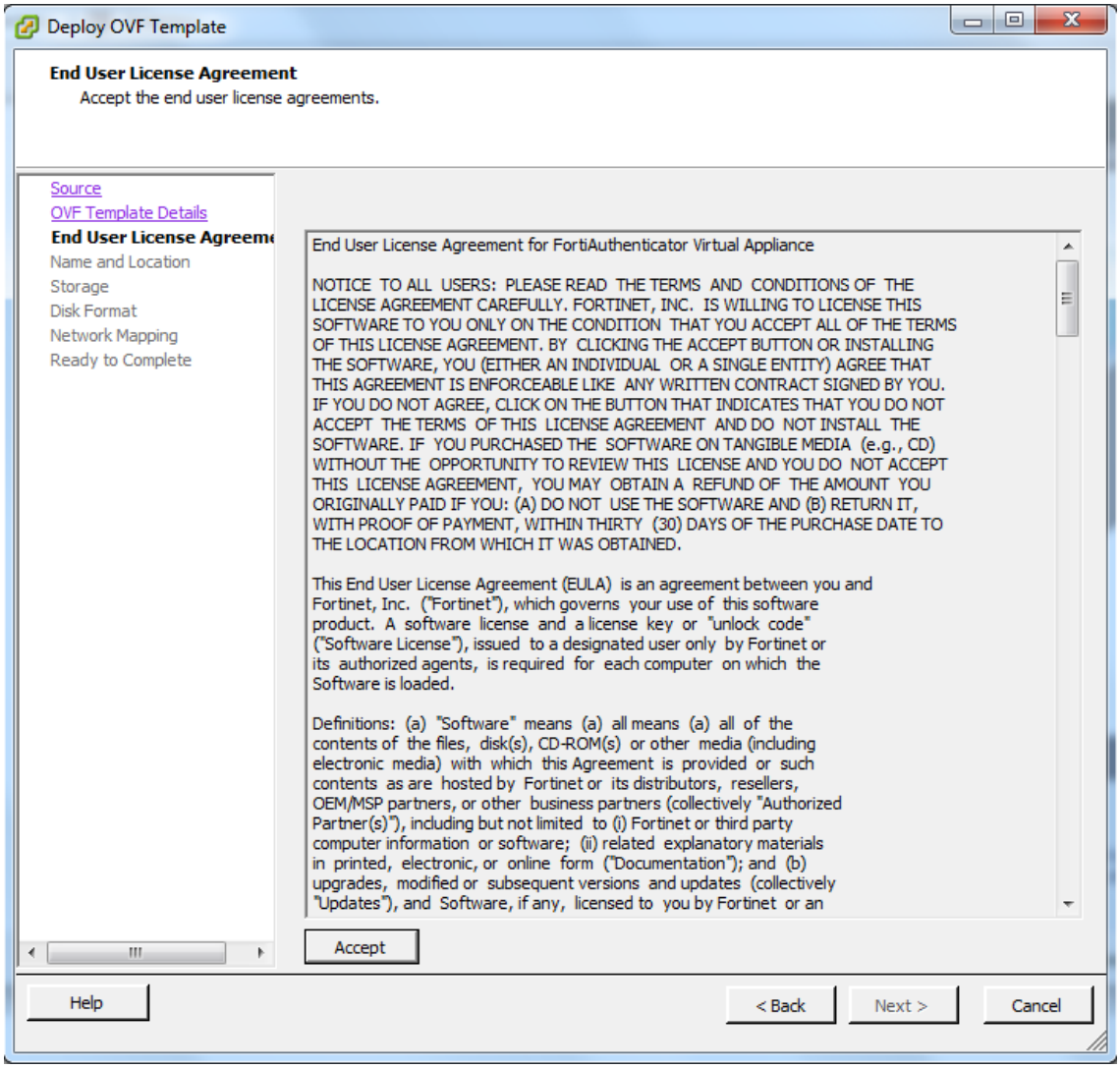
3. Select the source location of the OVF file. Select *Browse* and locate the OVF file on your computer. Select *Next* to continue.



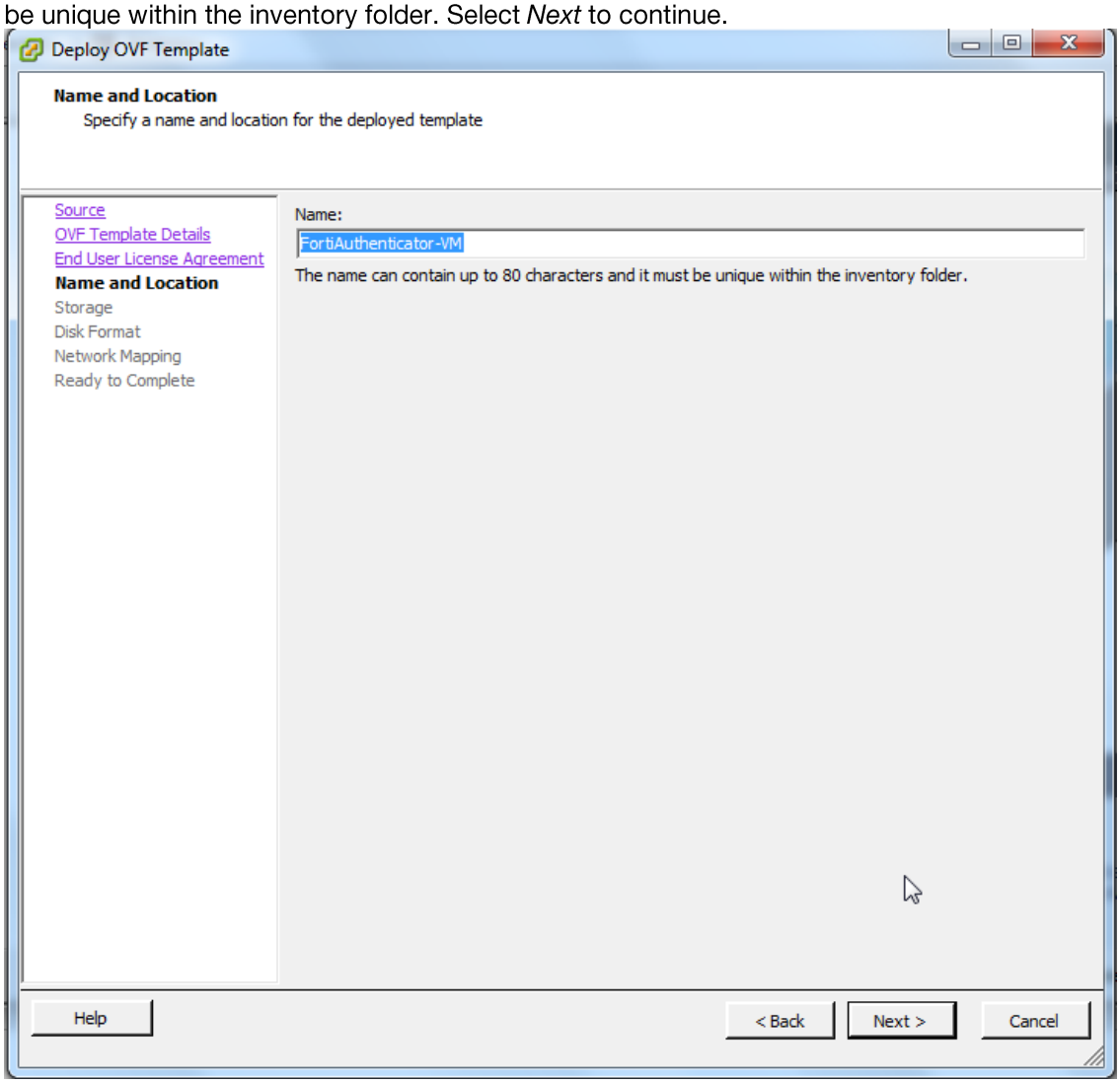
4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Select *Next* to continue.



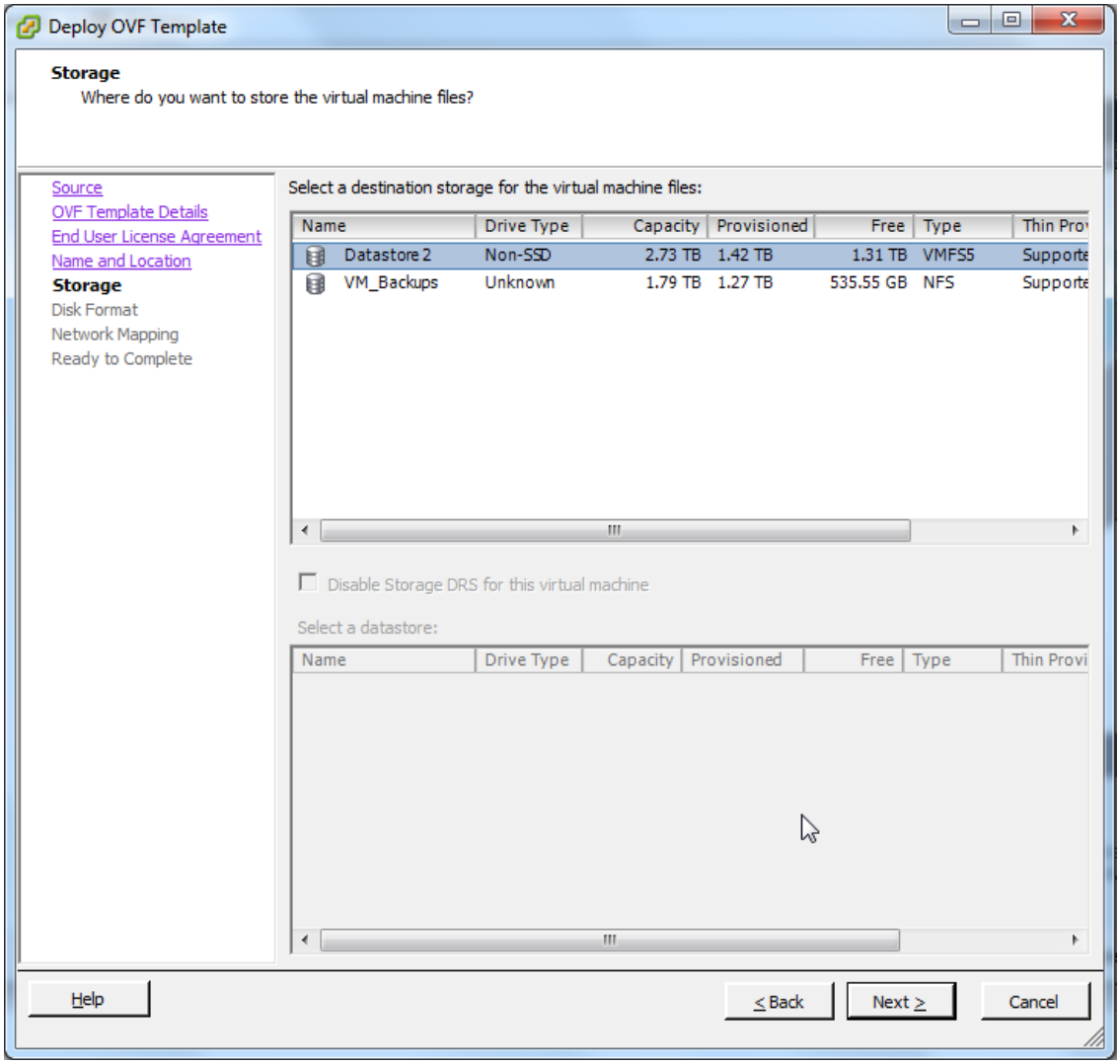
5. Read the end user license agreement for FortiAuthenticator VM. Select *Accept* and then select *Next* to continue.


Deploy OVF Template
End User License Agreement
Accept the end user license agreements.
Source
OVF Template Details
End User License Agreeme
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete
End User License Agreement for FortiAuthenticator Virtual Appliance
NOTICE TO ALL USERS: PLEASE READ THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT CAREFULLY. FORTINET, INC. IS WILLING TO LICENSE THIS SOFTWARE TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN CONTRACT SIGNED BY YOU. IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS LICENSE AGREEMENT AND DO NOT INSTALL THE SOFTWARE. IF YOU PURCHASED THE SOFTWARE ON TANGIBLE MEDIA (e.g., CD) WITHOUT THE OPPORTUNITY TO REVIEW THIS LICENSE AND YOU DO NOT ACCEPT THIS LICENSE AGREEMENT, YOU MAY OBTAIN A REFUND OF THE AMOUNT YOU ORIGINALLY PAID IF YOU: (A) DO NOT USE THE SOFTWARE AND (B) RETURN IT, WITH PROOF OF PAYMENT, WITHIN THIRTY (30) DAYS OF THE PURCHASE DATE TO THE LOCATION FROM WHICH IT WAS OBTAINED.
This End User License Agreement (EULA) is an agreement between you and Fortinet, Inc. ("Fortinet"), which governs your use of this software product. A software license and a license key or "unlock code" ("Software License"), issued to a designated user only by Fortinet or its authorized agents, is required for each computer on which the Software is loaded.
Definitions: (a) "Software" means (a) all means (a) all of the contents of the files, disk(s), CD-ROM(s) or other media (including electronic media) with which this Agreement is provided or such contents as are hosted by Fortinet or its distributors, resellers, OEM/MSP partners, or other business partners (collectively "Authorized Partner(s)"), including but not limited to (i) Fortinet or third party computer information or software; (ii) related explanatory materials in printed, electronic, or online form ("Documentation"); and (b) upgrades, modified or subsequent versions and updates (collectively "Updates"), and Software, if any, licensed to you by Fortinet or an
Accept
Help
< Back
Next >
Cancel

6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Select *Next* to continue.



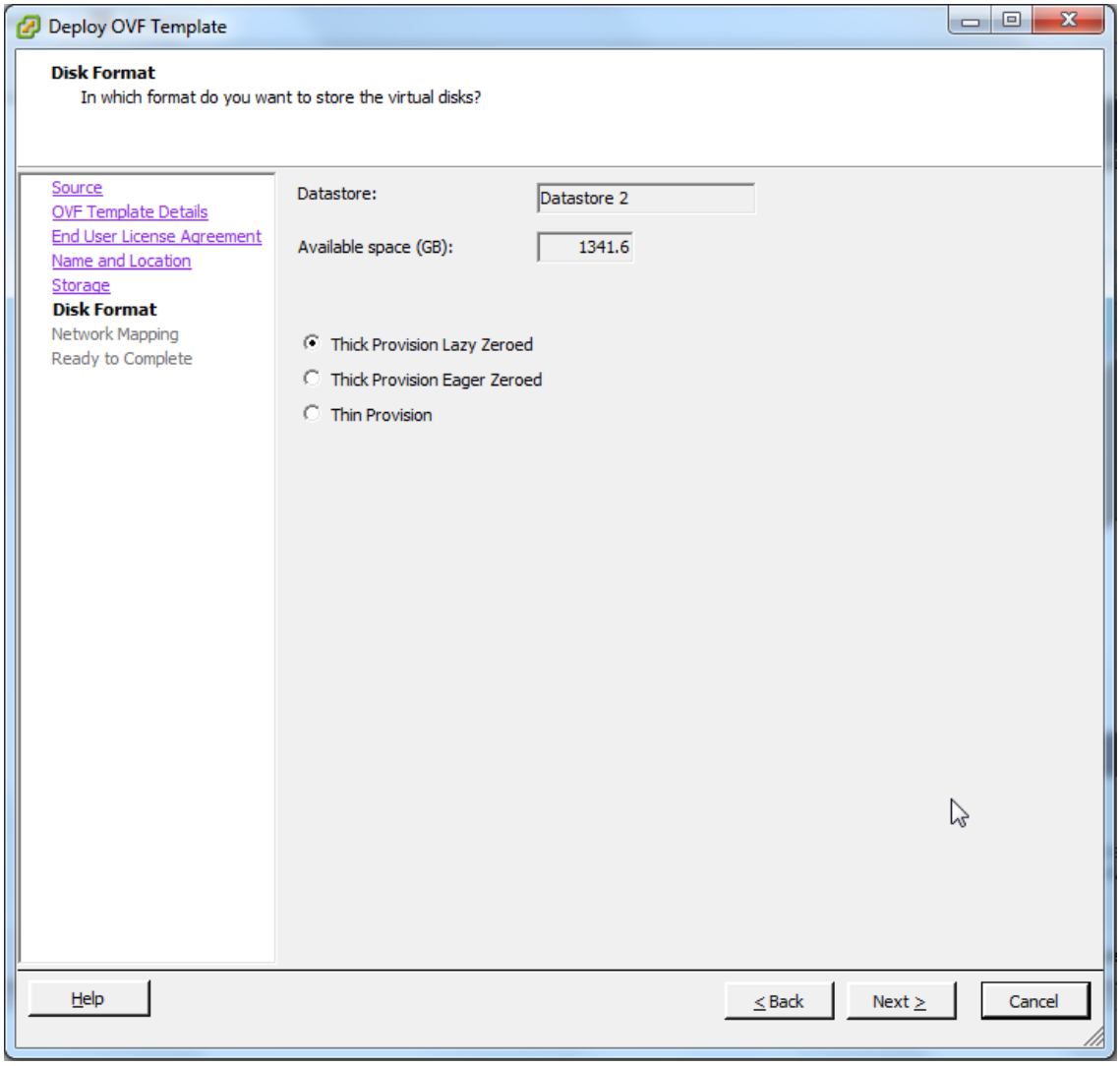
7. Select the Datastore into which the virtual machine is to be installed to. Select *Next* to continue.



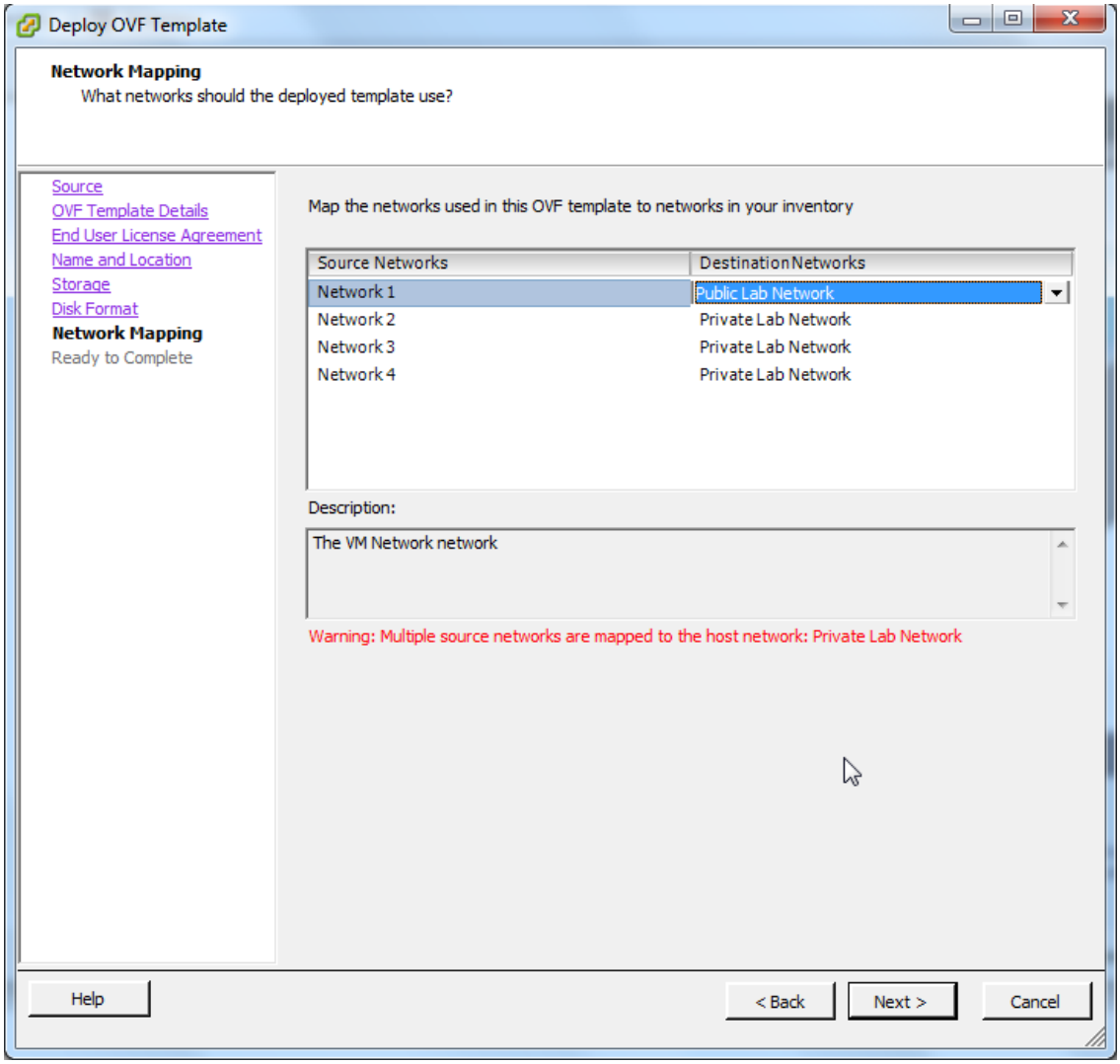
8. Select the preferred disk provisioning format:

- Thick Provision Lazy Zeroed: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
- Thick Provision Eager Zeroed: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
- Thin Provision: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains on the volume regardless if you have deleted data, etc.

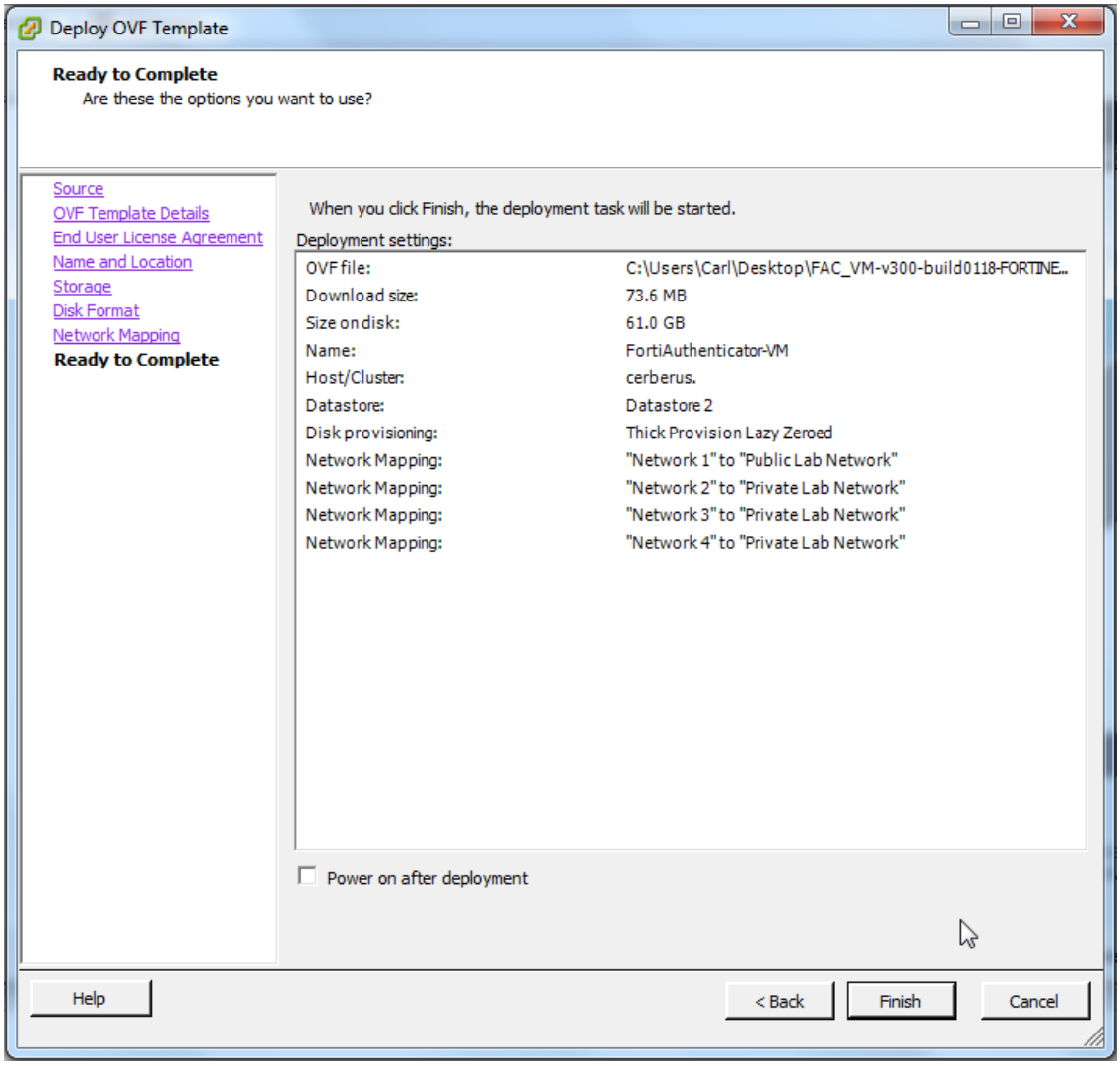
  Select *Next* to continue.



9. Map the networks used in this OVF template to networks in your inventory. Network1 maps to port1 of the FortiAuthenticator VM. You must set the destination network for this entry to access the device console. Select *Next* to continue.



10. Review the template configuration. Make sure that Power on after deployment is not enabled. You might need to configure the FortiAuthenticator VM hardware settings prior to powering on the FortiAuthenticator VM.



11. Select *Finish* to deploy the OVF template. You will receive a *Deployment Completed Successfully* dialog box once the FortiAuthenticator VM OVF template wizard has finished.

Configure FortiAuthenticator VM hardware settings

Before powering on your FortiAuthenticator VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiAuthenticator VM license. See Table 3 for FortiAuthenticator VM specification information.

Power on your FortiAuthenticator VM

You can now proceed to power on your FortiAuthenticator VM. There are several ways to do this:

- Select the name of the FortiAuthenticator VM you deployed in the inventory list and select Power on the virtual machine in the Getting Started tab.
- In the inventory list, right-click the name of the FortiAuthenticator VM you deployed, and select Power > Power On.

- Select the name of the FortiAuthenticator VM you deployed in the inventory list. Click the Power On button on the toolbar. Select the Console tab to view the console. To enter text, you must click in the console pane. The mouse is then captured and cannot leave the console screen. As the FortiAuthenticator console is text-only, no mouse pointer is visible. To release the mouse, press Ctrl-Alt.

Deployment example: MS Hyper-V

Once you have downloaded the .hyperv.zip file and extracted the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

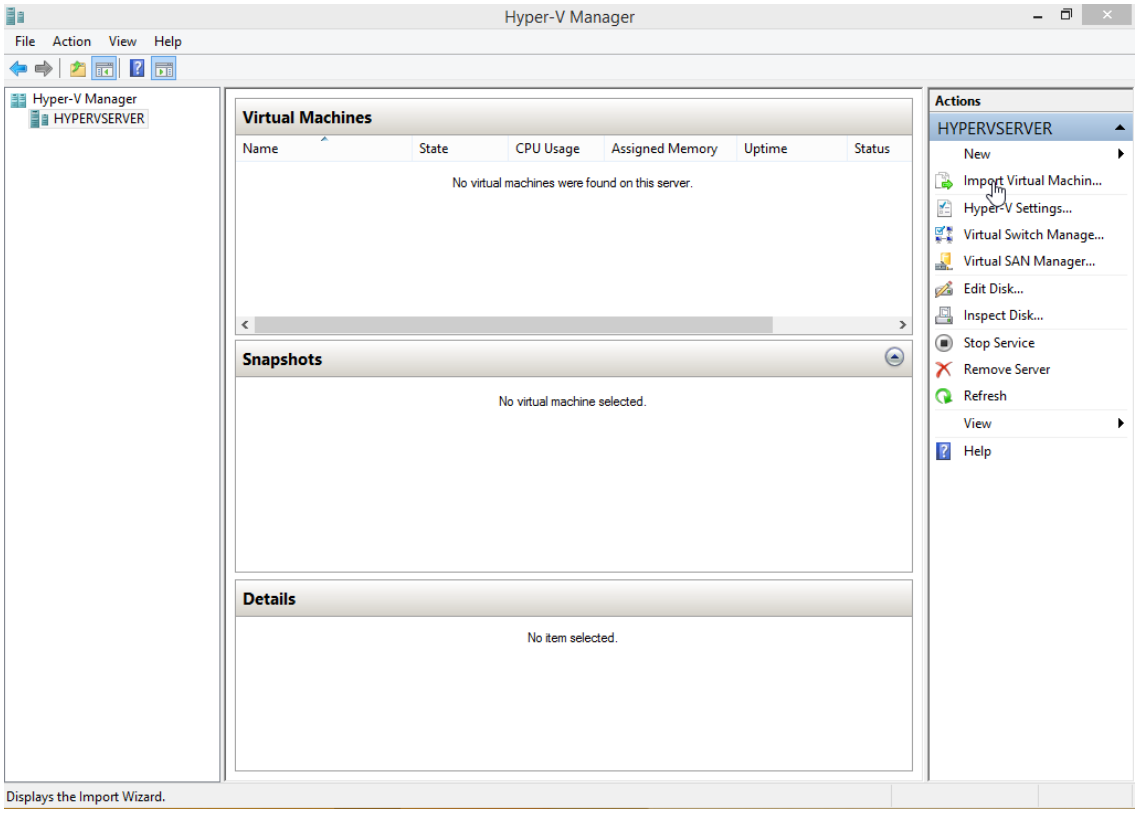
The following topics are included in this section:

- Create the FortiAuthenticator VM virtual machine
- Configure FortiAuthenticator VM hardware settings
- Start the FortiAuthenticator VM

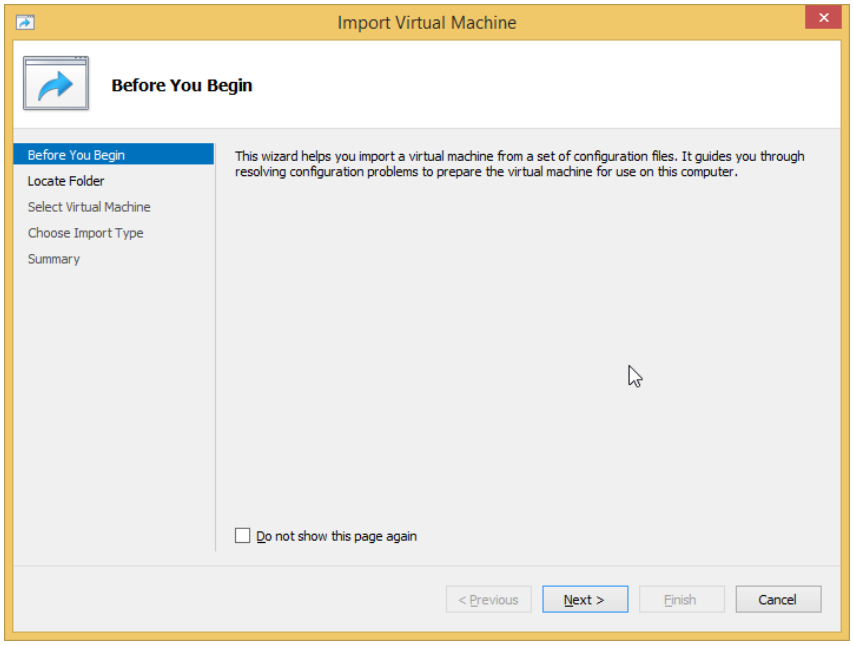
Create the FortiAuthenticator VM virtual machine

To create the FortiAuthenticator VM virtual machine:

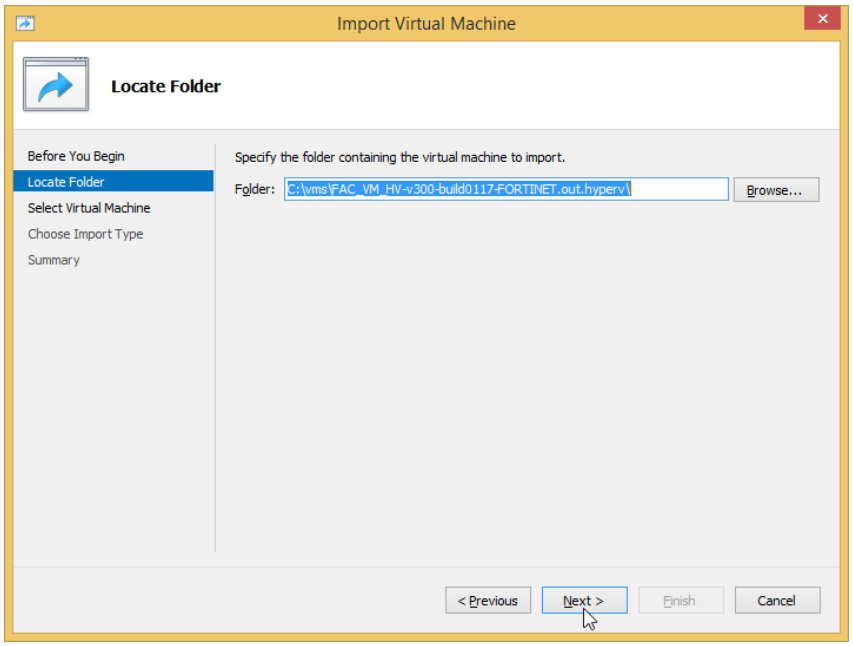
1. As an Administrator, launch the Hyper-V Manager and connect to your Hyper-V Server.
2. Select the server in the right hand-tree menu and Import Virtual Machine.



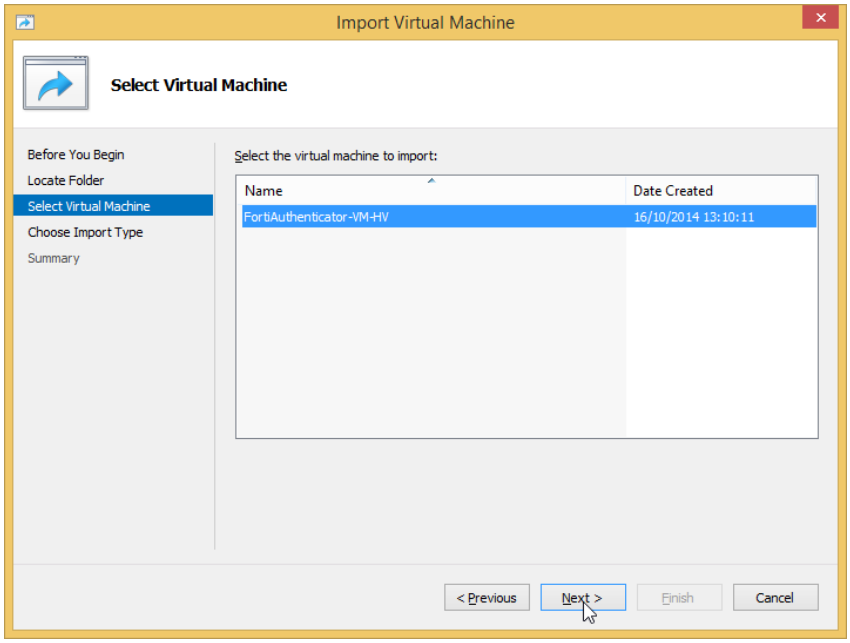
3. The Import Virtual Machine page opens, select *Next* to begin the VM Import process.



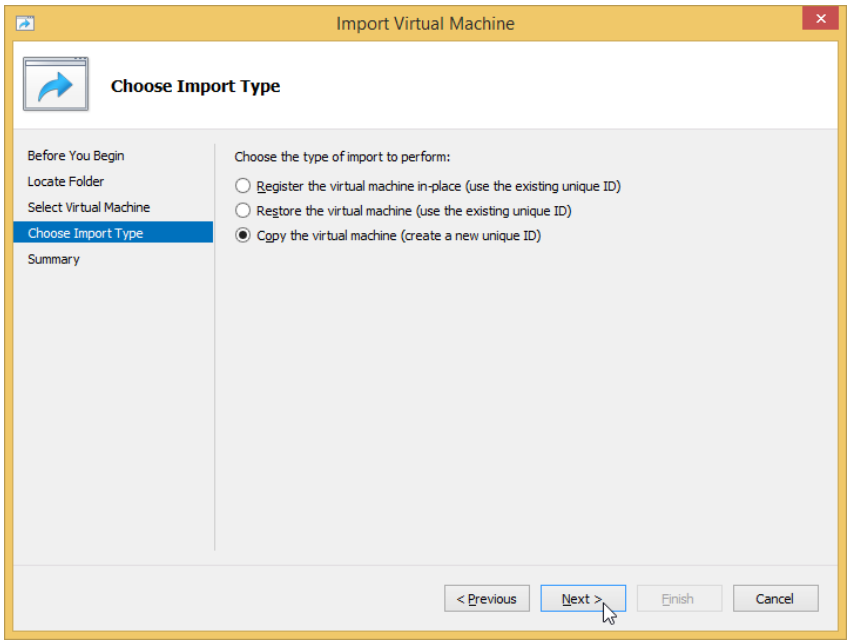
4. Enter the location of the VM to be imported. This is the location of the folder that you extracted the FortiAuthenticator hyperv.zip file to



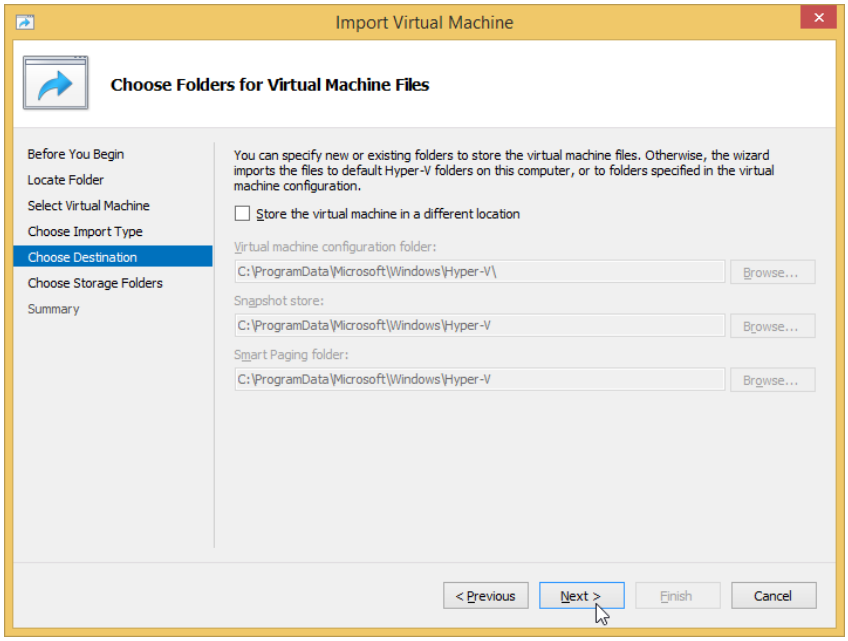
5. Select the FortiAuthenticator VM and select *Next*.



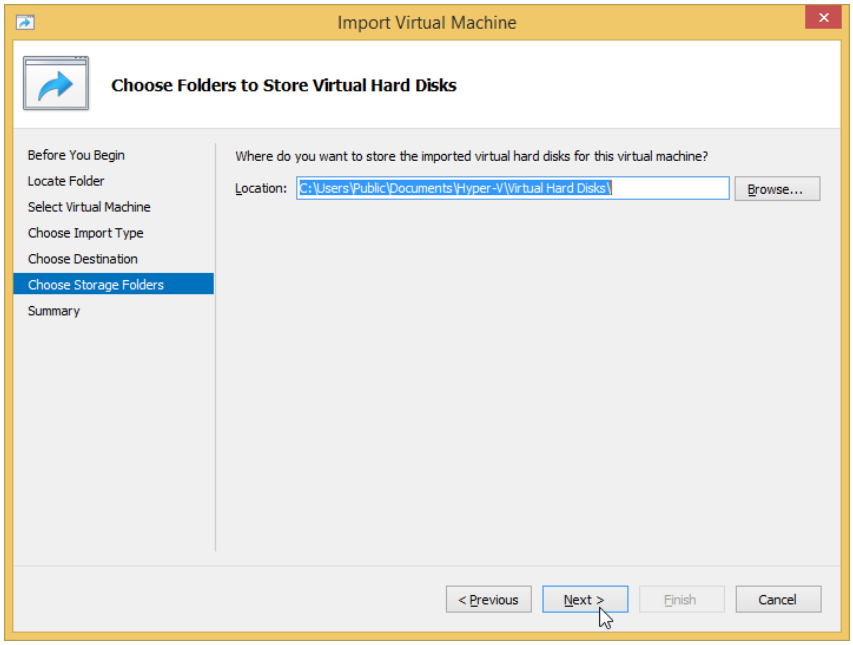
6. Chose the Import Type "*Copy the virtual machine*" and click *Next*.



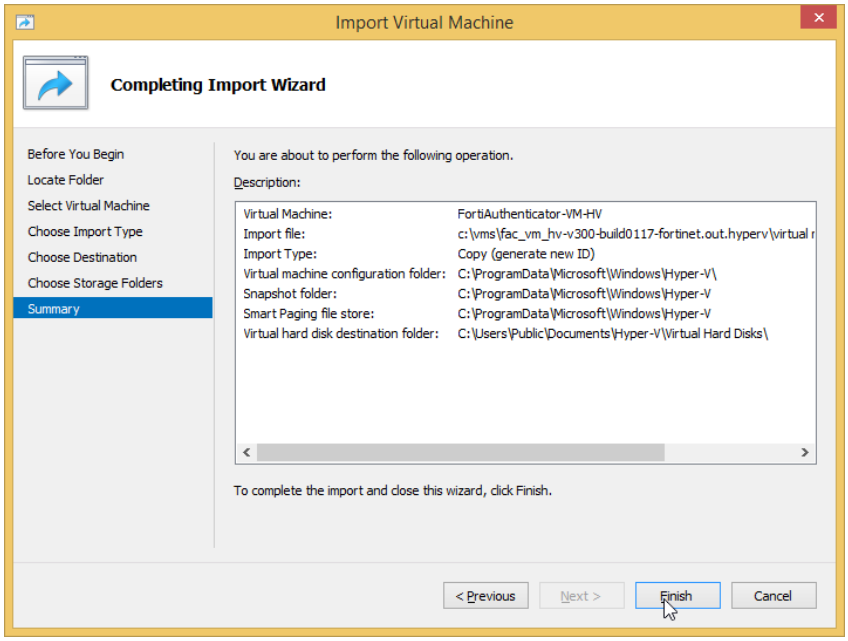
7. In the next steps, the default VM files storage locations can be modified, however for the purpose of this guide, the default settings will be accepted.



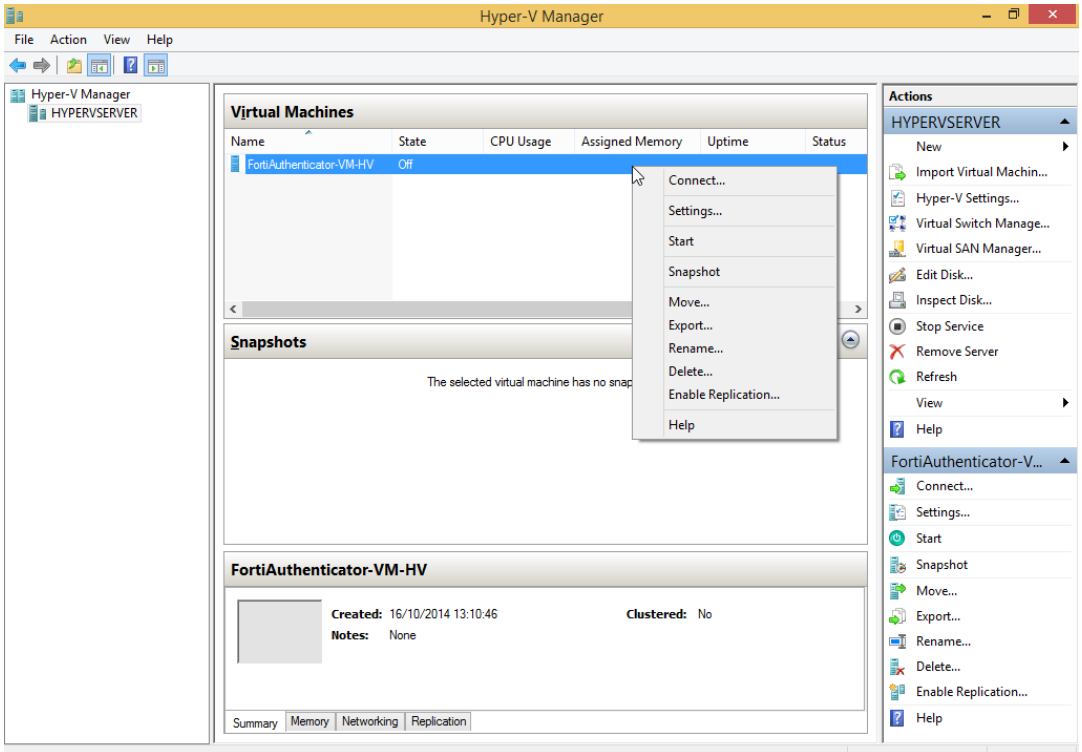
8. Similarly, the In the next steps, the default VM hard disk storage locations can be modified, however for the purpose of this guide, the default settings will be accepted.



9. Select Finish to accept the configuration and complete the VM installation.



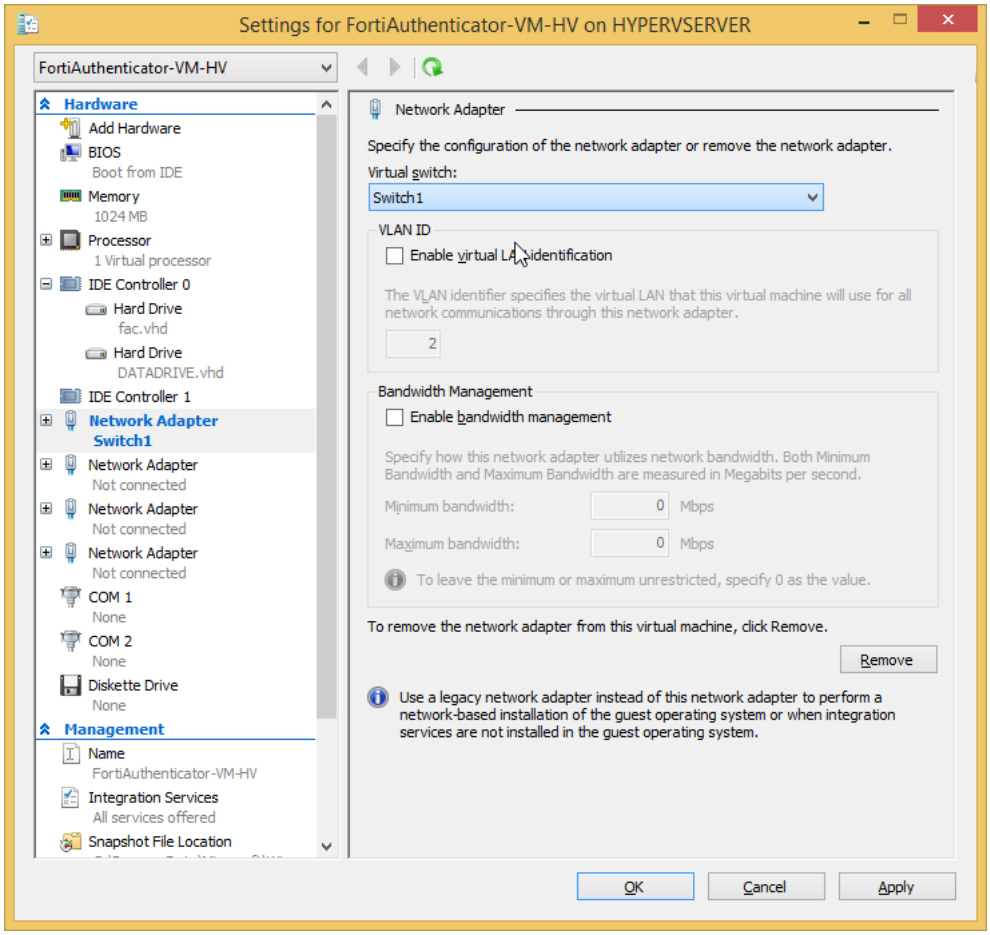
10. The VM will be installed and will be displayed in the Hyper-V Manager. Once complete, and before the VM is started, the hardware settings can be modified. Right mouse click the new VM and select *Settings*.



Configure FortiAuthenticator VM hardware settings

Before powering on your FortiAuthenticator VM you must configure the virtual memory, virtual CPU, and virtual disk configuration to match your FortiAuthenticator VM license. See Table 3 for FortiAuthenticator VM specification information.

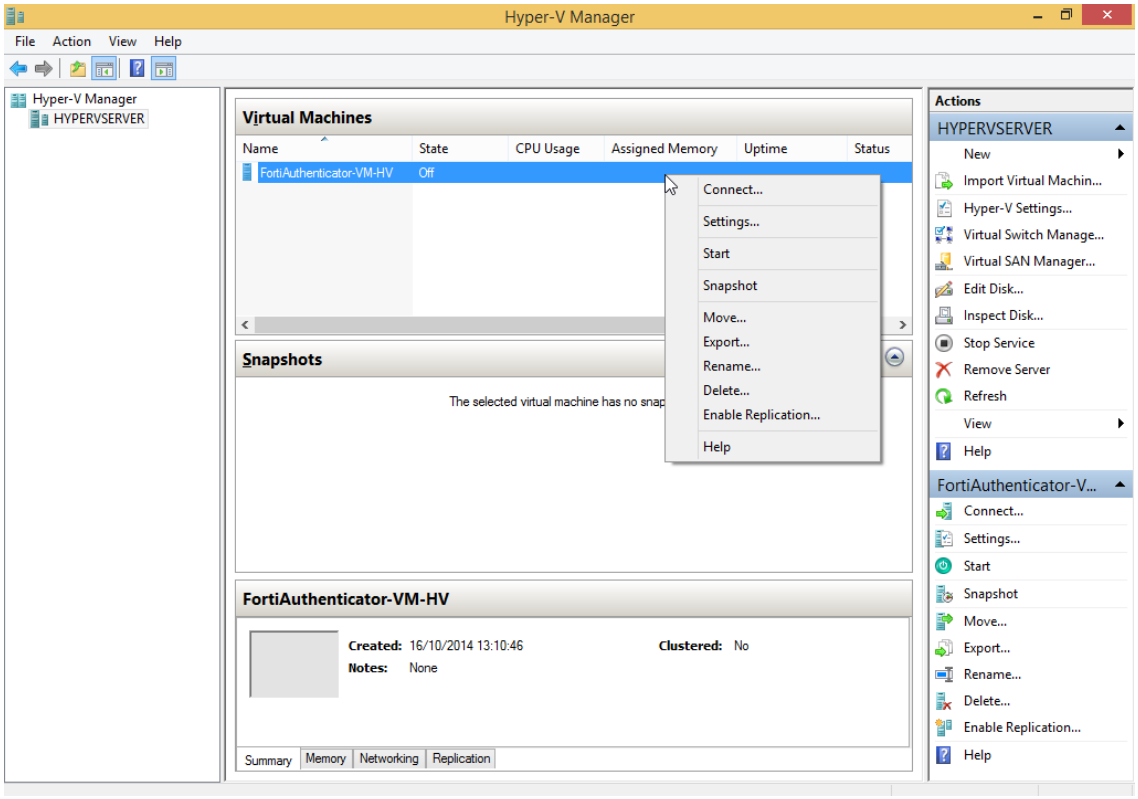
Select the virtual network adapters and assign them to the relevent virtual switches on your system. At this stage, make any modifications that may also be required to the CPU count and Memory. Select *OK* when completed.



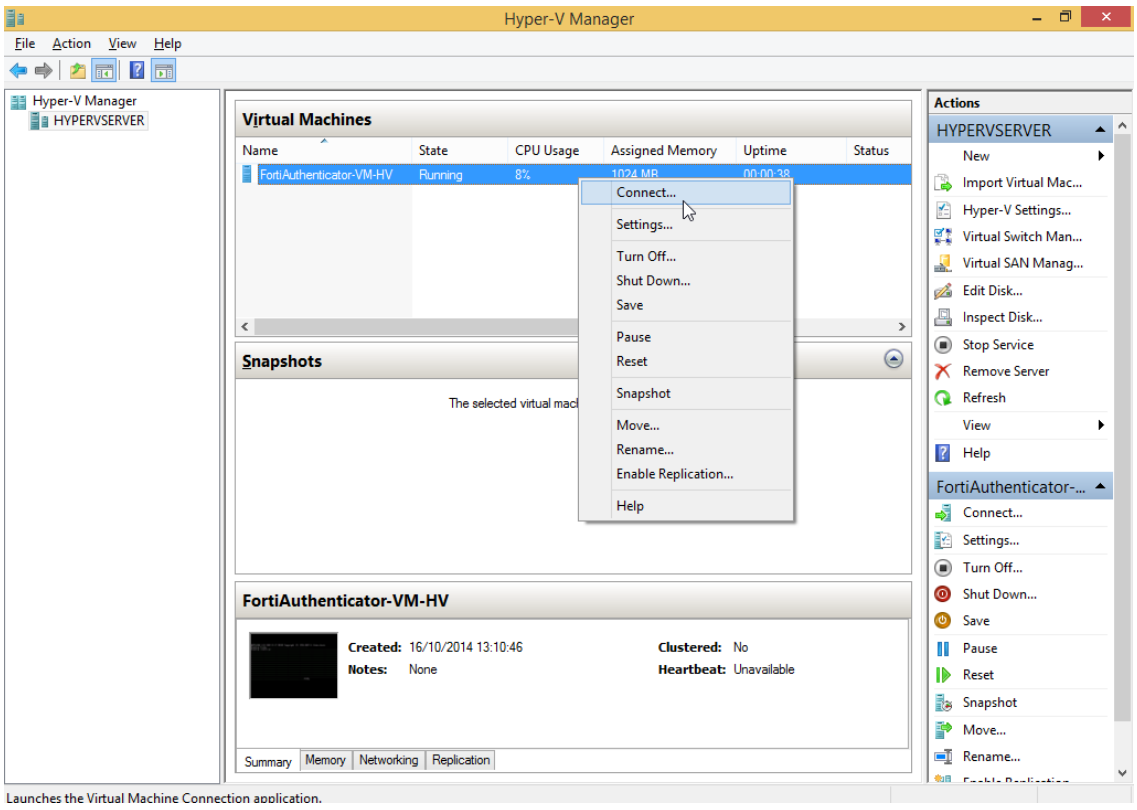
Power on your FortiAuthenticator VM

You can now proceed to power on your FortiAuthenticator VM. There are several ways to do this:

- Once nessesary modifications have been made, right click on the VM and select Start.



Once the VM has booted, connect to the console to configure the FortiAuthenticator VM for you network.



FortiAuthenticator VM Initial Configuration

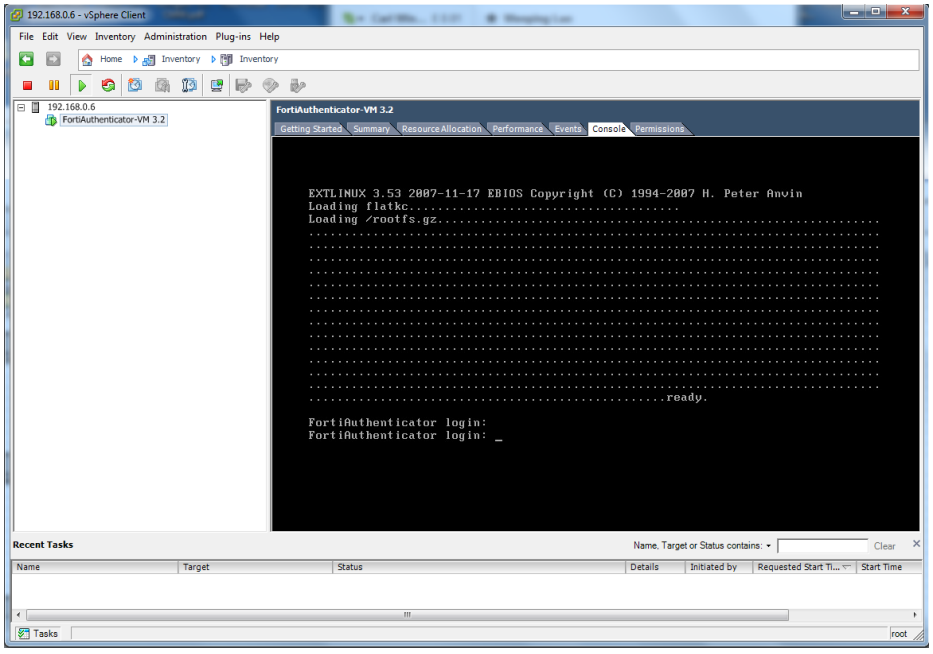
Before you can connect to the FortiAuthenticator VM web-based manager you must configure a network interface in the FortiAuthenticator VM console. Once an interface with administrative access is configured, you can connect to the FortiAuthenticator VM web-based Manager and upload the FortiAuthenticator VM license file that you downloaded from the Customer Service & Support website.

The following topics are included in this section:

- Set FortiAuthenticator VM port1 IP address
- Connect to the FortiAuthenticator VM Web-based Manager
- Upload the FortiAuthenticator VM license file
- Configure your FortiAuthenticator VM

Set FortiAuthenticator VM port1 IP address

Hypervisor management environments include a guest console window. On the FortiAuthenticator VM, this provides access to the FortiAuthenticator console, equivalent to the console port on a hardware FortiAuthenticator unit. Before you can access the Web-based manager, you must configure FortiAuthenticator VM port1 with an IP address and administrative access.



To configure the port1 IP address:

1. In your hypervisor manager, start the FortiAuthenticator VM and access the console window. You might need to press Return to see a login prompt.
2. Log in with the credentials *admin* and a blank password

3. Change the IP address using the command

```
Set port1-ip <ip>/<subnet mask>
Set default-gw <default gateway>
```

Connect to the FortiAuthenticator VM Web-based Manager

When you have configured the port1 IP address and netmask, launch a web browser and enter the IP address that you configured for port1. At the login page, enter the username admin and password field and select Login. The default password is blank.

Upload the FortiAuthenticator VM license file

FortiAuthenticator comes with a 5 user license. Before proceeding, upload the license that you received from the support site. This can be done under System > Administration > Licensing. This should be done before proceeding with any further configuration.

Configure your FortiAuthenticator VM

Once the FortiAuthenticator VM license has been validated you can begin to configure your device.

For more information on configuring your FortiAuthenticator VM see the FortiOS Handbook at

http://docs.fortinet.com/fortiauthenticator/admin-guides.